AMENDMENTS TO THE CLAIMS

THIS LISTING OF CLAIMS WILL REPLACE ALL PRIOR VERSIONS, AND LISTINGS OF CLAIMS IN THE APPLICATION.

LISTING OF CLAIMS:

1. (Currently amended) A method for detecting spurious network traffic comprising:

receiving a packet, the packet including data for transmission over a network;

determining an expected port for the packet~~, the expected port being a port~~ upon which the packet is expected to be received;

determining an actual port for the packet~~, the actual port being the port~~ upon which the packet is actually received;

comparing the actual port to the expected port; and

providing spurious packet handling when the actual port does not correspond to the expected port.

2. (Original) The method of claim 1 further comprising:

determining a plurality of expected ports for the packet; and

providing spurious packet handling when the actual port does not correspond to any one of the plurality of expected ports.

3. (Original) The method of claim 1 wherein spurious packet handling includes discarding the packet.

4. (Original) The method of claim 1 wherein spurious packet handling includes generating an alert.

5. (Original) The method of claim 1 wherein the packet comprises an Internet Protocol packet.

6. (Currently amended) The method of claim 1 wherein determining ~~an~~ the expected port for the packet further comprises:

determining a source network address for the packet; and

calculating an expected path for the packet according to ~~the~~ routing trees of ~~one or more~~ switches in the network, wherein an ending of the expected path is the ~~concluding with an~~ expected port.

7. (Original) The method of claim 1 wherein determining an expected port for the packet further comprises:

generating a table, the table associating each one of a plurality of source network addresses with a single port;

determining a source network address for the packet; and

applying the table to determine single port associated with the source network address, the single port being the expected port.

8. (Currently amended) A system for detecting spurious network traffic comprising:

receiving means for receiving a packet;

first determining means for determining an expected port for the packet;

second determining means for determining an actual port for the packet;

comparing means for comparing the expected port and the actual port; and

handling means for providing spurious packet handling ~~when~~ upon determining that the actual port does not correspond to the expected port.

9. (Original) The system of claim 8 further comprising:

third determining means for determining a plurality of expected ports for the packet; and

second handling means for providing spurious packet handling when the actual port does not correspond to any one of the plurality of expected ports.

10. (Currently amended) A switch for use in an internetwork, the switch comprising:

a plurality of ports, each port connected in a communicating relationship with at least one of a connected switch and a network;

a routing database, the routing database containing information relating to the internetwork; and

a processor, the processor configured to compare a first port ~~to a second port, the first port being a one~~ of the plurality of ports through which a packet is received to a ~~and the~~ second port ~~being a one~~ of the plurality of ports through which the packet is expected to be received, the processor further configured to provide spurious packet handling ~~when~~upon determining that the first port is different from the second port.

11. (Original) The switch of claim 10 wherein the routing database includes a routing tree for each one of a plurality of connected switches.

12. (Original) The switch of claim 10 wherein the routing database includes a plurality of link state update packets and a plurality of routing update packets.

13. (Original) The switch of claim 10 wherein the second port is calculated by examining one or more routing trees stored in the routing database.

14. (Currently amended) The switch of claim 10 wherein the second port is calculated by examining ~~the~~ a source network address of the packet.

15. (Original) The switch of claim 10 wherein the processor is further configured to generate an expected port table, the expected port table mapping each of a plurality of possible source network addresses to a unique port of the switch, whereby the second port is calculated by using a source network address of the packet to look up the second port.

16. (Original) The switch of claim 10 wherein the processor is further configured to generate an expected port table, the expected port table mapping each of a plurality of

possible source network addresses to a plurality of possible ports of the switch, whereby a plurality of possible second ports are calculated by using a source network address of the packet.

17. (Original) The switch of claim 16 wherein each one of the plurality of possible second ports has associated therewith a weight, the weight relating to a likelihood that the packet is received from the one of the plurality of possible second ports.

18. (Original) The switch of claim 10 wherein the spurious network traffic handling includes discarding the packet.

19. (Original) The switch of claim 10 wherein the spurious network traffic handling includes generating an alert.

20. (Currently amended) An internetwork comprising a plurality of switches, each of the switches comprising:

a plurality of ports, each port connected in a communicating relationship with at least one of a connected switch and a network;

a routing database, the routing database containing information relating to the internetwork; and

a processor, the processor configured to compare a first port ~~to a second port, the first port being a one~~ of the plurality of ports through which a packet is received to a ~~and the~~ second port ~~being a one~~ of the plurality of ports through which the packet is expected to be received, the processor further configured to provide spurious packet handling ~~when~~upon determining that the first port is different from the second port;

whereby spurious network traffic within the internetwork is detected.